MATH. SCAND. 43 (1978), 26–34

FIELDS GENERATED BY LINEAR COMBINATIONS OF ROOTS OF UNITY, II

R. J. EVANS and I. M. ISAACS

1. Introduction and notation.

In [1], the authors showed that under minor restrictions, a $\mathbf{Q}$-linear combination of complex roots of unity generates a field over which the field generated by those roots of unity involved has relatively small degree. In this paper, this degree is determined precisely for certain linear combinations of two and four roots of unity, using standard Galois theory. Specifically, let ζ_1 and ζ_2 be roots of unity and let $a, b \in \mathbf{Q}$ be nonzero. Define $\alpha = a\zeta_1 + b\zeta_2$ and $\beta = \alpha + \bar{\alpha}$. The object of this paper is to determine precisely the degrees

$$e = |\mathbf{Q}(\zeta_1, \zeta_2):\mathbf{Q}(\alpha)| \quad \text{and} \quad h = |\mathbf{Q}(\zeta_1, \zeta_2):\mathbf{Q}(\beta)| .$$

Our attempt to make such a determination for linear combinations of three roots of unity was not successful.

We fix some further notation. Let $k_i = O(\zeta_i)$, the order of ζ_i in the group of roots of unity. Let $d = (k_1, k_2)$ and let k be the least common multiple of k_1 and k_2. Write $\zeta = e^{2\pi i/k}$, so the ζ_i are powers of ζ and $\mathbf{Q}(\zeta_1, \zeta_2) = \mathbf{Q}(\zeta)$. If $(k, t) = 1$, let σ_t denote the unique automorphism in $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ such that $\sigma_t(\zeta) = \zeta^t$.

Since the fields $\mathbf{Q}(\alpha)$ and $\mathbf{Q}(\beta)$ remain unchanged if α or β is replaced by a nonzero rational multiple of itself, we assume that a and b are relatively prime integers. It suffices to consider the case $a, b > 0$, since $-\zeta_i$ is a root of unity. By symmetry, we may also assume $a \geqq b > 0$. The determination of $e = |\mathbf{Q}(\zeta):\mathbf{Q}(\alpha)|$ is made in Theorems 1 and 9 in the cases $a = b$ and $a > b$, respectively. The determination of h is made as follows. For a root of unity η, write $\gamma(\eta) = \eta + \eta^{-1}$ and let $\gamma_i = \gamma(\zeta_i)$, so $\beta = a\gamma_1 + b\gamma_2$. We have

$$h = |\mathbf{Q}(\zeta):\mathbf{Q}(\beta)| = |\mathbf{Q}(\zeta):\mathbf{Q}(\gamma(\zeta))| \cdot g \cdot f ,$$

where

$$g = |\mathbf{Q}(\gamma(\zeta)):\mathbf{Q}(\gamma_1, \gamma_2)|$$

Received September 12, 1977.

and

$$f = |\mathbf{Q}(\gamma_1, \gamma_2):\mathbf{Q}(\beta)| .$$

The factor $|\mathbf{Q}(\zeta):\mathbf{Q}(\gamma(\zeta))|$ is evaluated in Lemma 2 (a). The factor g is determined in Theorem 11. Finally, f is determined in Theorems 6 and 10 in the cases $a=b$ and $a>b$, respectively. We remark that in the course of proving Theorem 6, we obtain the following interesting result: $\cos\theta\cos\delta \in \mathbf{Q}(\cos\theta+\cos\delta)$ where θ, δ are rational multiples of π, unless $\cos\theta+\cos\delta=0$.

We shall use the following simple facts repeatedly. For roots of unity η, ξ, and $\lambda=\pm 1$, we have

$$\gamma(\xi)+\lambda\gamma(\eta) = \xi^{-1}(1+\lambda\xi\eta^{-1})(1+\lambda\xi\eta) \tag{1}$$

and hence

$$\gamma(\xi) = \lambda\gamma(\eta) \quad \text{iff} \quad \xi = \lambda\eta \quad \text{or} \quad \xi = \lambda\eta^{-1} . \tag{2}$$

Since the Galois group $\mathrm{Gal}\,(\mathbf{Q}(\zeta)/\mathbf{Q})$ is abelian, every field F such that $\mathbf{Q}(\zeta) \supset F \supset \mathbf{Q}$ is Galois over $\mathbf{Q}$. Furthermore, each element in $\mathrm{Gal}\,(F/\mathbf{Q})$ is the restriction to F of some element of $\mathrm{Gal}\,(\mathbf{Q}(\zeta)/\mathbf{Q})$.

2. The degrees e and f when $a=b$.

Write $\alpha=\zeta_1+\zeta_2$ and $\beta=\gamma_1+\gamma_2$. We first evaluate $e=|\mathbf{Q}(\zeta):\mathbf{Q}(\alpha)|$. If $\zeta_1 = \pm\zeta_2$, then either $\mathbf{Q}(\alpha)=\mathbf{Q}$ or $\mathbf{Q}(\alpha)=\mathbf{Q}(\zeta)$. We exclude these two simple cases in the following theorem.

THEOREM 1. *Let $\alpha=\zeta_1+\zeta_2$ and assume that $\zeta_1 \neq \pm\zeta_2$. Then $e\leqq 2$ with equality iff ζ_1 and ζ_2 are interchanged by some element of* $\mathrm{Gal}\,(\mathbf{Q}(\zeta)/\mathbf{Q})$.

PROOF. We have $\zeta_1^{-1}+\zeta_2^{-1}=\bar{\alpha} \in \mathbf{Q}(\alpha)$. Also, $\bar{\alpha}\zeta_1\zeta_2=\alpha$. Since $\bar{\alpha}\neq 0$, it follows that $\zeta_1\zeta_2 \in \mathbf{Q}(\alpha)$ and thus the polynomial $f(X)=(X-\zeta_1)(X-\zeta_2)$ has coefficients in $\mathbf{Q}(\alpha)$. Thus $e\leqq 2$ with equality iff $f(X)$ is irreducible over $\mathbf{Q}(\alpha)$. Since $\zeta_1\neq\zeta_2$, equality occurs iff ζ_1 and ζ_2 are interchanged by some automorphism of $\mathbf{Q}(\zeta)=\mathbf{Q}(\zeta_1,\zeta_2)$.

To evaluate $f=|\mathbf{Q}(\gamma_1,\gamma_2):\mathbf{Q}(\beta)|$, we shall need the following lemmas.

LEMMA 2. *Let η be a root of unity of order n. Then*

a) $$|\mathbf{Q}(\eta):\mathbf{Q}(\gamma(\eta))| = \begin{cases} 2 & \text{if } n>2 \\ 1 & \text{if } n\leqq 2 \end{cases}$$

b) $$\mathbf{Q}(\gamma(\eta)) = \mathbf{Q}(\eta) \cap \mathbf{R} .$$

PROOF. Part (a) follows since the polynomial $(X-\eta)(X-\eta^{-1})$ has coefficients in $\mathbf{Q}(\gamma(\eta))$. Part (b) follows since $\mathbf{Q}(\eta) \supseteq \mathbf{Q}(\eta) \cap \mathbf{R} \supseteq \mathbf{Q}(\gamma(\eta))$ and $\eta \notin \mathbf{R}$ for $n>2$.

LEMMA 3. *We have*

$$|\mathbf{Q}(\gamma_1) \cap \mathbf{Q}(\gamma_2):\mathbf{Q}| = \begin{cases} \varphi(d)/2 & \text{if } d>2 \\ 1 & \text{if } d \leqq 2, \end{cases}$$

where $d=(k_1,k_2)$.

PROOF. It is well known that $\mathbf{Q}(\zeta_1) \cap \mathbf{Q}(\zeta_2) = \mathbf{Q}(e^{2\pi i/d})$. Intersecting this with $\mathbf{R}$ and applying Lemma 2, we obtain the result.

For integers $n>1$, we define $\Lambda(n)=p$ if n is a power of some prime p and $\Lambda(n)=1$ otherwise. The following lemma is easily proved [2, p. 507].

LEMMA 4. *Let η be a root of unity of order $n>1$. Then $\Lambda(n)$ is the product of the distinct algebraic conjugates of $1-\eta$.*

LEMMA 5. *Let ξ and η be roots of unity with $\gamma(\xi) \neq \gamma(\eta)$ and suppose $a \in \mathbf{Z}$ divides $\gamma(\xi)-\gamma(\eta)$ in the ring of algebraic integers. Then*

$$a^{\varphi(u)\varphi(v)} \text{ divides } \Lambda(u)^{\varphi(v)}\Lambda(v)^{\varphi(u)}$$

(in $\mathbf{Z}$) where $u=O(\xi\eta)$ and $v=O(\xi\eta^{-1})$.

PROOF. By (2) we have $u,v>1$ and so $\Lambda(u)$ and $\Lambda(v)$ are defined. Let $N:\mathbf{Q}(\xi,\eta) \to \mathbf{Q}$ be the norm map and let $|\mathbf{Q}(\xi,\eta):\mathbf{Q}|=m$. It follows from (1) that

$$a^m \text{ divides } N(\xi^{-1}(1-\xi\eta)(1-\xi\eta^{-1})).$$

Since $N(\xi^{-1})=\pm 1$, Lemma 4 yields that a^m divides $\Lambda(u)^{m/\varphi(u)}\Lambda(v)^{m/\varphi(v)}$ and the result follows.

We now evaluate $f=|\mathbf{Q}(\gamma_1,\gamma_2):\mathbf{Q}(\beta)|$. If $\gamma_1=\pm\gamma_2$, then either $\mathbf{Q}(\beta)=\mathbf{Q}$ or $\mathbf{Q}(\beta)=\mathbf{Q}(\gamma_1,\gamma_2)$. We exclude these two simple cases in the next theorem.

THEOREM 6. *Let $\beta=\gamma_1+\gamma_2$ and assume that $\gamma_1 \neq \pm\gamma_2$. Then $f \leqq 2$ with equality iff γ_1 and γ_2 are interchanged by some element of* Gal $(\mathbf{Q}(\zeta)/\mathbf{Q})$.

PROOF. Let $F=\mathbf{Q}(\beta,\gamma_1\gamma_2)$ and $f_0=|\mathbf{Q}(\gamma_1,\gamma_2):F|$. Since the polynomial $p(X)=(X-\gamma_1)(X-\gamma_2)$ has coefficients in F, it follows that $f_0 \leqq 2$ with equality iff $p(X)$

is irreducible over F. Since $\gamma_1 \neq \gamma_2$, we see that $p(X)$ is irreducible (and $f_0 = 2$) iff γ_1 and γ_2 are interchanged by some element of $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$. It therefore suffices to show that $f = f_0$, i.e., that $\gamma_1\gamma_2 \in \mathbf{Q}(\beta)$.

CASE 1. $k_1 = k_2 = k$.

First suppose that $3 \nmid k$. Then

$$\begin{aligned}\beta^3 &= (\gamma_1)^3 + (\gamma_2)^3 + 3\beta\gamma_1\gamma_2 \\ &= (\gamma(\zeta_1^3) + 3\gamma_1) + (\gamma(\zeta_2^3) + 3\gamma_2) + 3\beta\gamma_1\gamma_2 \\ &= \sigma_3(\beta) + 3\beta(1 + \gamma_1\gamma_2)\,.\end{aligned}$$

Since $\sigma_3(\beta) \in \mathbf{Q}(\beta)$, it follows that $\gamma_1\gamma_2 \in \mathbf{Q}(\beta)$ as desired.

Now suppose that $3 \mid k$. Write $m = k/3$ and choose $c \in \{1+m, 1-m\}$ such that $3 \nmid c$. Then $(k, c) = 1$ and $\sigma_c(\beta) \in \mathbf{Q}(\beta)$. We have $\zeta_1^{c-1} = \omega$ where ω is some primitive cube root of 1. Without loss of generality, $\zeta_2^{c-1} = \omega$, otherwise replace ζ_2 by ζ_2^{-1}. Then $\sigma_c(\beta) = \omega\alpha + \bar{\omega}\bar{\alpha}$ and $\mathbf{Q}(\beta, \omega)$ contains $\sigma_c(\beta) - \bar{\omega}\beta = (\omega - \bar{\omega})\alpha$. Thus $\alpha \in \mathbf{Q}(\beta, \omega)$. We have $|\mathbf{Q}(\beta, \omega) : \mathbf{Q}(\beta)| = 2$ and thus

$$|\mathbf{Q}(\zeta) : \mathbf{Q}(\beta)| \leqq 2|\mathbf{Q}(\zeta) : \mathbf{Q}(\alpha)|\,.$$

Since $|\mathbf{Q}(\zeta) : \mathbf{Q}(\gamma_1, \gamma_2)| \geqq 2$, this yields

$$f_0 \leqq f = |\mathbf{Q}(\gamma_1, \gamma_2) : \mathbf{Q}(\beta)| \leqq |\mathbf{Q}(\zeta) : \mathbf{Q}(\alpha)| = e\,.$$

Since $\gamma_1 \neq \pm\gamma_2$, we have $\zeta_1 \neq \pm\zeta_2$ by (2); thus, by Theorem 1, $e \leqq 2$ with equality iff ζ_1 and ζ_2 are interchanged by some $\tau \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$. It follows that if $f_0 \neq f$, then $f_0 = 1$, $f = e = 2$, and ζ_1 and ζ_2 are interchanged by some τ. Then τ interchanges γ_1 and γ_2 which implies that $f_0 = 2$, a contradiction. Thus $f = f_0$ and this completes the proof in Case 1.

CASE 2. $2d \mid k_1$ or $2d \mid k_2$, where $d = (k_1, k_2)$.

We may assume that $2d \mid k_2$. Write $n = k/2$ and note that $k_1 \mid n$. Choose $c \in \{1, 2\}$ such that $2 \nmid (n + c)$. Then $(k, n + c) = 1$ and $\sigma_{n+c}(\beta) \in \mathbf{Q}(\beta)$. Since $\zeta_1^n = 1$ and $\zeta_2^n = -1$, we have

$$\begin{aligned}\sigma_{n+c}(\beta) &= \zeta_1^c + \zeta_1^{-c} - (\zeta_2^c + \zeta_2^{-c}) \\ &= \gamma(\zeta_1^c) - \gamma(\zeta_2^c)\,.\end{aligned}$$

If $c = 1$, this yields $\gamma_1 - \gamma_2 \in \mathbf{Q}(\beta)$ and thus $\gamma_1, \gamma_2 \in \mathbf{Q}(\beta)$ as desired.

Suppose that $c = 2$. Since $\gamma_i^2 = \gamma(\zeta_i^2) + 2$, we have

$$(\gamma_1)^2 - (\gamma_2)^2 = \sigma_{n+2}(\beta) \in \mathbf{Q}(\beta)\,.$$

Therefore,

$$\gamma_1 - \gamma_2 = (\gamma_1^2 - \gamma_2^2)/\beta \in \mathbf{Q}(\beta)$$

and thus $\gamma_1, \gamma_2 \in \mathbf{Q}(\beta)$. This completes the proof in Case 2.

We may now suppose that

$$k_1 < k_2, \quad 2d \nmid k_1 \quad \text{and} \quad 2d \nmid k_2 . \tag{3}$$

Assume that $\gamma_1\gamma_2 \notin \mathbf{Q}(\beta)$ and choose $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ such that $\sigma(\beta) = \beta$ and $\sigma(\gamma_1\gamma_2) \neq \gamma_1\gamma_2$. Then σ fixes neither γ_1 nor γ_2. In particular, $\gamma_i \notin \mathbf{Q}$ and so

$$\varphi(k_i) \geqq 4 \quad \text{for } i = 1, 2 . \tag{4}$$

Since σ fixes β, we have

$$\gamma_1 - \sigma(\gamma_1) = -(\gamma_2 - \sigma(\gamma_2)) \neq 0 . \tag{5}$$

We conclude by Case 1, with $\gamma_i - \sigma(\gamma_i)$ in place of β, that for $i = 1, 2$,

$$|\mathbf{Q}(\gamma_i - \sigma(\gamma_i)) : \mathbf{Q}| \in \{\varphi(k_i)/2, \varphi(k_i)/4\} . \tag{6}$$

If $\gamma_i \neq -\sigma(\gamma_i)$, then $\varphi(k_i)/4$ is taken in (6) iff γ_i and $-\sigma(\gamma_i)$ are interchanged by an element of $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$.

CASE 3. $k_1 \mid k_2$.

By (3), $k_2 \neq 2k_1$ and hence $\varphi(k_1) < \varphi(k_2)$. Thus, using (5) and (6), we have

$$\begin{aligned} \varphi(k_1)/2 &= |\mathbf{Q}(\gamma_1 - \sigma(\gamma_1)) : \mathbf{Q}| \\ &= |\mathbf{Q}(\gamma_2 - \sigma(\gamma_2)) : \mathbf{Q}| = \varphi(k_2)/4 . \end{aligned} \tag{7}$$

Since $k_1 \mid k_2$, it follows from (3) and (7) that $k_2 = 3k_1$ and $3 \nmid k_1$. Since the value $\varphi(k_2)/4$ is taken in (6) when $i = 2$, we conclude that

$$\gamma_2 \neq -\sigma(\gamma_2) \tag{8}$$

and that there exists $\tau \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ which interchanges γ_2 and $-\sigma(\gamma_2)$. Therefore, by (2) we have $\tau(\zeta_2) = -\sigma(\zeta_2)^{\pm 1}$ and $\tau(\sigma(\zeta_2)) = -\zeta_2^{\pm 1}$. It follows that $\tau(\zeta_2^3) = -\sigma(\zeta_2^3)^{\pm 1}$ and $\tau(\sigma(\zeta_2^3)) = -(\zeta_2^3)^{\pm 1}$ and thus τ interchanges $\gamma(\zeta_2^3)$ and $-\sigma(\gamma(\zeta_2^3))$. Since ζ_2^3 is conjugate to ζ_1, we conclude that τ interchanges γ_1 and $-\sigma(\gamma_1)$. By (7) and the remark immediately following (6), we conclude that $\gamma_1 = -\sigma(\gamma_1)$.

By (5),

$$2\gamma_1 = -(\gamma_2 - \sigma(\gamma_2)) \tag{9}$$

and since $\gamma(\sigma(\zeta_2))=\sigma(\gamma_2)\neq\gamma_2$, Lemma 5 yields

$$2^{\varphi(u)\varphi(v)} \text{ divides } \Lambda(u)^{\varphi(v)}\Lambda(v)^{\varphi(u)} \tag{10}$$

where $u=O(\zeta_2\sigma(\zeta_2))>1$ and $v=O(\zeta_2^{-1}\sigma(\zeta_2))>1$. Since $\sigma(\zeta_2)=\zeta_2^w$ for some w and $O(\zeta_2)=k_2$, we have

$$u = k_2/(k_2, w+1) \quad \text{and} \quad v = k_2/(k_2, w-1)\,.$$

It follows that one of u or v is divisible by 3 and the corresponding value of Λ is 1 or 3. It now follows from (10) that one of $\varphi(u)$ or $\varphi(v)$ is 1 and so one of u or v is 2. Therefore, $\sigma(\zeta_2)=-\zeta_2^{\pm 1}$ and thus $\sigma(\gamma_2)=-\gamma_2$. This contradicts (8) and the proof in Case 3 is complete.

CASE 4. $k_1 \nmid k_2$.

By (5) we have

$$\gamma_i-\sigma(\gamma_i) \in \mathbf{Q}(\gamma_1) \cap \mathbf{Q}(\gamma_2)$$

and thus by Lemma 3

$$|\mathbf{Q}(\gamma_i-\sigma(\gamma_i)):\mathbf{Q}| \text{ divides } \begin{cases} \varphi(d)/2 & \text{if } d>2 \\ 1 & \text{if } d\leqq 2\,. \end{cases} \tag{11}$$

Suppose $d\leqq 2$. By (6) and (11), $\varphi(k_i)\leqq 4$ for $i=1,2$ and by (4), $\varphi(k_1)=4=\varphi(k_2)$. This implies that $k_1, k_2 \in \{5,8,10,12\}$, which contradicts (3).

Thus $d>2$. For some $i\in\{1,2\}$, assume that $\gamma_i-\sigma(\gamma_i)$ has degree $\varphi(k_i)/2$ over $\mathbf{Q}$. Then (11) yields $\varphi(k_i)\leqq\varphi(d)$. Since $d\,|\,k_i$, we have $k_i=d$ or $k_i=2d$ which contradicts (3) and the fact that $k_1\nmid k_2$.

Therefore, by (6), $\gamma_i-\sigma(\gamma_i)$ has degree $\varphi(k_i)/4$ over $\mathbf{Q}$ for each $i\in\{1,2\}$. Thus $\varphi(k_i)$ divides $2\varphi(d)$ by (11). Since $\varphi(d)$ divides $\varphi(k_i)$, we have $\varphi(k_i)\in\{\varphi(d), 2\varphi(d)\}$ and thus $k_i/d\in\{1,2,3,4,6\}$ for each i. This contradicts (3) and the fact that $k_1\nmid k_2$, and the proof of the theorem is complete.

Write $\zeta_1=\zeta^r$ and $\zeta_2=\zeta^s$. In the following corollaries to Theorems 1 and 6, we show how e and f may be computed in terms of k, r and s. The proofs are straightforward and are omitted.

COROLLARY 7. *Assume that* $\zeta_1\neq\pm\zeta_2$. *Then* $e\leqq 2$ *with equality iff*

$$(k, rs) = 1 \quad \textit{and} \quad r^2 \equiv s^2 (\mathrm{mod}\, k)\,.$$

COROLLARY 8. *Assume that* $\gamma_1\neq\pm\gamma_2$. *Then* $f\leqq 2$ *with equality iff*

$$(k, rs) = 1 \quad \textit{and} \quad r^2 \equiv \pm s^2 (\mathrm{mod}\, k)\,.$$

3. The degrees e and f when $a>b$.

We have $\alpha=a\zeta_1+b\zeta_2$, $\beta=a\gamma_1+b\gamma_2$ where $(a,b)=1$, $a>b>0$. In Theorems 9 and 10 below, e and f are determined. We omit the proof of Theorem 9, as it is very similar to that of Theorem 10. We note that Theorem 9 is much more complicated to prove than Theorem 1, the corresponding theorem in the case $a=b$.

THEOREM 9. *We have $e\leqq 2$ with equality iff*

$$k_1 = 3k_2,\ 3\nmid k_2,\ 4\mid k_2\,,$$

$$b = 1,\ a = 2,\ \text{and}\ \zeta_1 = \omega^{\pm 1}\zeta_2$$

where $\omega=e^{2\pi i/3}$. If $e=2$, then α is fixed by the automorphism $\sigma\in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ defined by $\sigma(\zeta_2)=-\zeta_2$ and $\sigma(\omega)=\omega^{-1}$.

THEOREM 10. *We have $f\leqq 2$ with equality iff*

$$k_1 = 3k_2,\ 3\nmid k_2,\ 4\mid k_2,\ k_2>4\,, \tag{12}$$

$$b = 1,\ a = 2,\ \text{and}\ \zeta_1 = \omega^{\pm 1}\zeta_2^{\pm 1}$$

where $\omega=e^{2\pi i/3}$. If $f=2$, then β is fixed by the automorphism $\sigma\in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ defined by $\sigma(\zeta_2)=-\zeta_2$ and $\sigma(\omega)=\omega^{-1}$.

PROOF. If (12) holds, it is easily checked that $\sigma(\beta)=\beta$ but that $\sigma(\gamma_2)=-\gamma_2\neq\gamma_2$ and thus

$$f = |\mathbf{Q}(\gamma_1,\gamma_2):\mathbf{Q}(\beta)| \geqq 2\,.$$

Now suppose that $\tau\in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ and that τ fixes β but does not fix both γ_1 and γ_2. It remains to show that (12) holds and that $\tau(\gamma_i)=\sigma(\gamma_i)$ for $i=1,2$.

Since $\tau(\beta)=\beta$, we have

$$(-a/b)(\gamma_1-\tau(\gamma_1)) = (\gamma_2-\tau(\gamma_2)) \neq 0\,. \tag{13}$$

Note that $k_2>4$ and $k_2\neq 6$, or else $\gamma_2\in\mathbf{Q}$ and $\tau(\gamma_2)-\gamma_2=0$, a contradiction. By (13), a divides $\gamma_2-\tau(\gamma_2)$ in the ring of algebraic integers and thus Lemma 5 yields

$$a^{\varphi(u)\varphi(v)} \text{ divides } \Lambda(u)^{\varphi(v)}\Lambda(v)^{\varphi(u)} \tag{14}$$

where $u=O(\tau(\zeta_2)\zeta_2)$ and $v=O(\tau(\zeta_2)\zeta_2^{-1})$.

Write $\tau(\zeta_2)=\zeta_2^w$ for some w with $(k_2,w)=1$. Thus $u=k_2/(k_2,w+1)$ and $v=k_2/(k_2,w-1)$.

First suppose that $u=v$. Then

$$(k_2, w+1) = (k_2, w-1)\,. \tag{15}$$

Since $(w+1, w-1) \leqq 2$, it follows that $u=v \in \{k_2, k_2/2\}$. It is therefore impossible that $u=v=2$ or $u=v=3$ since $k_2>4$ and $k_2 \neq 6$. If $u=v=4$, then $k_2=8$, w is odd and exactly one of $w+1$ and $w-1$ is divisible by 4. This contradicts (15). We conclude that

$$\text{if } u = v, \text{ then } u \geqq 5\,. \tag{16}$$

Next, suppose that $u>2$ and $v>2$. Since each of $\Lambda(u)$ and $\Lambda(v)$ is either 1 or prime and since $a>1$, it follows from (14) that $\varphi(u)\varphi(v) \leqq \varphi(u)+\varphi(v)$. Since $\varphi(u), \varphi(v)>1$, it follows that $\varphi(u)=2=\varphi(v)$ and by (14), $\Lambda(u)=\Lambda(v) \neq 1$. Thus u and v are powers of the same prime and so $u=v \in \{3,4\}$. This contradicts (16). We conclude that one of u or v is 2 and that $u \neq v$.

Let x be the one of u or v different from 2. Then by (14), $a^{\varphi(x)}$ divides $2^{\varphi(x)}\Lambda(x)$. Since $\Lambda(x)$ is 1 or prime and since $\varphi(x)>1$, it follows that $a=2$ and $b=1$. Also, since one of u, v is even, we have $2 \mid k_2$ and $2 \nmid w$. Thus $2 \mid (k_2, w \pm 1)$ and therefore $4 \mid k_2$. Since moreover one of $u=O(\tau(\zeta_2)\zeta_2)$ or $v=O(\tau(\zeta_2)\zeta_2^{-1})$ is 2, we have $\tau(\zeta_2)=-\zeta_2^{\pm 1}$ and thus $\tau(\gamma_2)=-\gamma_2$. It now remains to complete the proof of (12) for then it will follow from the equalities $\tau(\gamma_2)=-\gamma_2=\sigma(\gamma_2)$ and $\tau(\beta)=\beta=\sigma(\beta)$ that $\tau(\gamma_1)=\sigma(\gamma_1)$.

Since $\tau(\gamma_2)=-\gamma_2$, (13) yields

$$\gamma_2 = (\tau(\gamma_1)-\gamma_1) \tag{17}$$

and thus $\mathbf{Q}(\gamma_2)=\mathbf{Q}(\gamma_1) \cap \mathbf{Q}(\gamma_2)$. Since $\gamma_2 \notin \mathbf{Q}$, it follows from Lemmas 2 and 3 that

$$\varphi(k_2) = \varphi(d)$$

where $d=(k_1, k_2)>2$. Since $d \mid k_2$ and $4 \mid k_2$, we conclude that $d=k_2$ and thus $k_2 \mid k_1$.

Since $\tau(\gamma_1) \neq \gamma_1$, Theorem 6 yields $|\mathbf{Q}(\tau(\gamma_1)-\gamma_1):\mathbf{Q}| \in \{\varphi(k_1)/2, \varphi(k_1)/4\}$ and hence by (17) we have either $\varphi(k_2)=\varphi(k_1)$ or $2\varphi(k_2)=\varphi(k_1)$. Assume that $\varphi(k_2)=\varphi(k_1)$. Since $k_2 \mid k_1$ and $4 \mid k_2$, it follows that $k_1=k_2$. Then $\gamma_2-\tau(\gamma_2)$ and $\gamma_1-\tau(\gamma_1)$ are algebraic conjugates and this is impossible by (13). Thus $\varphi(k_1)=2\varphi(k_2)$ and hence either $k_1=2k_2$ or $k_1=3k_2$ where the latter possibility can occur only if $3 \nmid k_2$. If $k_1=2k_2$, then σ_{1+k_2} negates γ_1 and fixes γ_2. This is impossible by (13) and we conclude that $k_1=3k_2$ and $3 \nmid k_2$.

It remains to prove that $\zeta_1=\omega^{\pm 1}\zeta_2^{\pm 1}$. We can certainly write $\zeta_1=\omega^y\zeta_2^z$ for some $y, z \in \mathbf{Z}$ where $y=\pm 1$ and $(k_2, z)=1$. Also, we have $\tau(\zeta_2)=-\zeta_2^{\lambda}$ and $\tau(\omega)=\omega^{\mu}$ where $\lambda, \mu \in \{1, -1\}$. Suppose $\lambda=\mu$. It follows that $\tau(\zeta_1)=-\zeta_1^{\lambda}$ and $\tau(\gamma_1)=-\gamma_1$. Thus (17) yields $\mathbf{Q}(\gamma_1)=\mathbf{Q}(\gamma_2)$, which contradicts the fact that $k_1=3k_2$. Thus $\lambda=-\mu$ and $\tau(\gamma_1)=-(\omega^y\zeta_2^{-z}+\omega^{-y}\zeta_2^z)$ and

$$\gamma_1 - \tau(\gamma_1) = (\omega^y + \omega^{-y})(\zeta_2^z + \zeta_2^{-z}) = -\gamma(\zeta_2^z) .$$

Then from (17), we obtain $\gamma_2 = \gamma(\zeta_2^z)$ and $\zeta_2 = \zeta_2^{\pm z}$ by (2). Thus $\zeta_1 = \omega^y \zeta_2^z = \omega^y \zeta_2^{\pm 1}$ and the proof is complete.

4. The degree g.

THEOREM 11. *Let* $g = |\mathbf{Q}(\gamma(\zeta)) : \mathbf{Q}(\gamma_1, \gamma_2)|$. *Then* $g \leqq 2$ *with equality iff* $(k_1, k_2) \leqq 2$, $k_1 > 2$ *and* $k_2 > 2$.

PROOF. The theorem is trivial when either $k_1 \leqq 2$ or $k_2 \leqq 2$ and so we assume $k_1 > 2$, $k_2 > 2$. We compute the order of $H = \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}(\gamma_1, \gamma_2))$ and observe that $g = |H|/2$ by Lemma 2 (a).

We have $\sigma_t \in H$ iff $\sigma_t(\gamma_i) = \gamma_i$ for $i = 1, 2$, i.e. iff

$$t \equiv \pm 1 \pmod{k_1} \quad \text{and} \quad t \equiv \pm 1 \pmod{k_2} . \tag{18}$$

For each of the four choices of sign in (18) there is at most one $t \pmod{k}$ satisfying (18), since if both t_1 and t_2 satisfy (18), then $k_1 \mid (t_1 - t_2)$ and $k_2 \mid (t_1 - t_2)$ and so $k \mid (t_1 - t_2)$. It follows that $|H| \leqq 4$ and hence $g \leqq 2$.

Since $\sigma_1, \sigma_{-1} \in H$, it follows that $g = 2$ iff there exists t such that

$$t \equiv -1 \pmod{k_1} \quad \text{and} \quad t \equiv 1 \pmod{k_2} . \tag{19}$$

(Note that any such t automatically satisfies $(k, t) = 1$.) Thus $g = 2$ iff $(k_1, k_2) \mid 2$.

REFERENCES

1. R. J. Evans and I. M. Isaacs, *Fields generated by linear combinations of roots of unity*, Trans. Amer. Math. Soc. 229 (1977), 249–258.
2. H. Hasse, *Zahlentheorie*, 2. erweiterte Auflage, Akademie-Verlag, Berlin, 1963.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA, SAN DIEGO
LA JOLLA, CALIFORNIA 92093

AND

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF WISCONSIN
MADISON, WISCONSIN 53706